内部統制との融合による リスクマネジメントの新展開

—リスクマネジメントにおける内部統制の意義について—

専修大学商学部　杉野文俊

Merger of Risk Management and Internal Control: Role of Internal Control in Enterprise Risk Management

Senshu University, School of Commerce Fumitoshi Sugino

米国においては「内部統制の統合的枠組み」（COSO1）が「全社的リスクマネジメント」（COSO2）となり，わが国においては内部統制の法制化（新会社法と金融商品取引法）が実現するなど，リスクマネジメントと内部統制の関係はかつてなく重要なものとなっている。その背景には内部監査とリスクマネジメントのそれぞれにおいて起きたパラダイムのシフトがあった。内部監査はリスクアプローチ型へ，リスクマネジメントは価値創造型への転換であったが，両者には通底するものがある。さらに直接的に両者を結合させたものはコーポレートガバナンスである。それは英国や日米におけるコーポレートガバナンス強化の動きにみるとおりである。米国における事例研究の文献をもとに，両者の関係は「融合」ともいうべきものであることを導出する。リスクマネジメントは内部統制の付加価値を高めるものであり，内部統制の法制化はリスクマネジメントの定着を促進させるものである。

キーワード：内部統制，リスクマネジメント，内部監査，パラダイムシフト，融合，コーポレートガバナンス

The COSO has published *Internal Control-Integrated Framework* in 1992 and *Enterprise Risk Management-Integrated Framework* in 2004. In Japan, two laws have been enacted regarding internal control. These represent merger of risk management and internal control. There were paradigm shift in risk management and internal audit, both of which are in line with each other resulting from the same change of business environment and the necessity for stronger corporate governance. The relationship between risk management and internal control has become even more important nowadays. Risk management will enhance the value of internal control and internal control will expedite adoption of enterprise risk management by Japanese corporations. This paper will examine the relationship between risk management and internal control relying on the case study in U.S.A. so as to conclude that the relationship should be characterized as merger.

Keywords：internal control, risk management, internal audit, paradigm shift, merger, corporate governance

1. はじめに

リスクマネジメントの古典的なテキストによれば，内部統制とは「会計士を直接リスクマネジメントに巻き込むものである」と言及されているに過ぎなかった（William & Heins, 1976，邦訳，p. 49）。その後，リスクマネジメントと内部統制のそれぞれにつき大きな発展があり，さらには「企業不祥事の防止」という現代企業社会の要請もあり，両者の関係はかつてないほど緊密で重要なものになっている。

一般的には内部統制はリスクマネジメントの一部であるとされる[1)]。また以前であれば，会計分野におけるリスクマネジメントであるともいえたであろう。しかし現代におけるリスクマネジメントと内部統制の関係は，それだけではないのではないか。その意味するところと背景を明らかにすることによって，リスクマネジメントと内部統制を実践するための指針が見出せるのではないか。そうした問題意識から，両者の関係について考察するのがこの論文の目的である。

リスクマネジメントと内部統制の関係が分かりにくい理由の１つは内部統制という用語自体がきわめて多義的であり[2)]，論者によってさまざまな

意味で使用されるからである。たとえば全社的リスクマネジメント（Enterprise Risk Management: ERM）のテキストであるDeLoach（2000, p. 24）にも，内部統制をリスクコントロール，とくに損失制御の意味で使用していると思われる箇所がある[3]。

これはやや極端な例としても，内部統制を「企業の資産を保全し，会計記録の正確性と信頼性を確保し，かつ，経営活動を総合的に計画し，調整し，評定するために，経営者が設定した制度・組織・方法および手続を総称するもの」（日本会計研究学会，1960年）であるとすれば[4]，「内部統制はリスクマネジメントにほかならない」としてもそれほどの違和感は生じない[5]。

この論文における内部統制は事実上の国際標準となっている「内部統制の統合的枠組み」（以下COSO1[6]）において提示されたものである。COSO1では，リスクマネジメントはその構成要素の一つであったが，同じトレッドウェイ委員会組織委員会による「全社的リスクマネジメント」（COSO2）では逆にリスクマネジメントの枠組みの中における内部統制とされるに至った。COSO 1とCOSO2の関係については，どう理解すればよいのか。それがリスクマネジメントと内部統制の「融合」であり，それには内部監査におけるパラダイムシフトが深く関係している。

内部監査はもともと内部統制の一部であり，他の統制の有効性を評価・保証するものである（松井，2006, p. 27）。それは監査役監査や公認会計士監査とは違い，「執行の側で，執行のために行われる」という特徴がある（鳥羽，2005, p. 173）。米国などの先進的な企業において，内部監査人がERMの導入を担ったという事実は，わが国におけるERMの可能性を考える上で示唆するところが大である。米国における事例研究の知見に依拠してそれらの点を論じていく。

副題を「リスクマネジメントにおける内部統制の意義について」とした。問題は「両者の関係」であるから「内部統制におけるリスクマネジメントの意義について」でもよいのであるが，わが国では内部統制によってERMの定着が促進されるであろうとの結論が導かれるので，そのような副題とした。

2. リスクマネジメントと内部監査のパラダイムシフト

2-1. リスクマネジメントのパラダイムシフト

リスクマネジメントにおいては，1990年代に，伝統的なリスクマネジメントから現代的なリスクマネジメントへと変化するパラダイムのシフトがあった。従来のパラダイムは，純粋リスクを中心としたものであるのに対し，新しいパラダイムでは，投機的リスクも対象とするのが大きな相違点である（Rejda, 2005, p. 63）。

純粋リスクとは損失のみを発生させるリスクであり，投機的リスクとは利益を生むこともあるリスクである。保険がもっぱら前者のリスクをカバーするものであることから，有用なリスクの分類方法であった[7]。リスクマネジメントが保険リスクに限られるものでないことは言うまでもないが，従来のリスクマネジメントは，主にリスクのマイナス面を管理するものであった。

現代的リスクマネジメントでは，投機的リスクのようにマイナスとプラスの影響があるリスクについて，リスクとは損失の可能性と同時に，利得の機会（opportunity）でもあると認識し，リスクと機会をリンクさせて（DeLoach, 2000），リスクマネジメントを事故対策という後向きのものから，イノベーションと成長のためのプロセス（業務活動）という前向きのものにする（Culp, 2001, p. 209）。すなわち伝統的なリスクマネジメントの目的は「損失の防止」もしくは「倒産の防止」であったのに対して，現代的リスクマネジメントではそれが「価値創造」と「競争力の源泉」であるという違いである。

リスクの定義については「新聞で毎日12回リスクという言葉を見れば，12通りの意味がある」（McNamee, 1998, p. 2），リスクの定義には実にさまざまなものがあるので「文脈において理解するしかない」（Culp, 2001, p. 15）とも言われる。たとえばRejda（2005, p. 3, p. 18）は「損失の

発生に関する不確実性」という定義を採用した上で，そのほかに5つの例を挙げている。現代的リスクマネジメントにおいては定義の統一を試みる動きもあり，ISOの用語委員会による定義[8]やリスクマネジメント規格（後述）もある。この論文では「組織体の目標と目的に重大な影響を及ぼす事象と結果の不確実性」[9]としておきたい。キーワードは「事象（event）」「結果（outcome）」そして「不確実性（uncertainty）[10]」である。

現代的リスクマネジメントとは，Enterprise-Wide Risk Management（EWRM），Enterprise Risk Management（ERM），Integrated Risk Management, Holistic Risk Management, Total Risk Managementなどの名称で提唱されているものであるが，この論文ではERM（全社的リスクマネジメント）という呼び名を使用する。これらの名称が示すとおり，現代的リスクマネジメントには「リスクの統合的な処理」と「全社的なリスクマネジメント」という2つの側面がある。

リスクの統合的な処理は，保険と金融の融合によって，また金融リスクのリスクマネジメントにおいて発達した手法である（Doherty, pp. 3–15）。純粋リスクと投機的リスクを，あるいはさまざまなビジネスリスク[11]を，組み合わせて処理することによって，個々のリスクに関する許容水準，リスクコスト，リスク資本の配分などを改善して，全体としてのリスクの最適化[12]を図ることができる。リスクを統合的に処理するためには，①すべてのリスクが見えていること，②現業部門（subject matter expert）を関与させること，③リスク分析を行うこと，そして④リスクの比較ができることが条件である（Walker et al., 2002, pp. 24–26）。

全社的なリスクマネジメントとは，リスクマネジメントを機能，部門，文化横断的なものにすることである（DeLoach, 2000, p. 5）。従来は，保険，財務，ITリスクなどの別に，それぞれの部門ごとに管理していたが，それらを全社的な観点から総合的・包括的に取り扱うことである。さらに特定の部署や社員の職務ではなく，部門・階層の如何を問わず，全社員が参加するものであるということである。

ERMの特徴で際立っているのは，リスクマネジメントは事業体の価値創造にかかわるものである，それ故リスクマネジメントは事業戦略と一体のものでなければならないとする「戦略整合性」の考え方である。それは下記の定義にも見るとおりである。

「EWRMとは事業体の価値創造にかかわる不確実性を評価し，管理するために，戦略，プロセス，人，技術，知識を整合させる構造的かつ規律のとれたアプローチである」（DeLoach, 2000, p. 5）

もう一つの特徴は，環境の変化によって生じる新しいリスクにも，場当たり的ではない，計画的な対応ができるということである。それは経験則からは測定のできないリスク，すなわち不確実性

図表1

リスクマネジメントのパラダイムシフト

旧パラダイム	新パラダイム
経営管理の一部	経営戦略と一体化
純粋リスク	投機的リスク
物的資産・財務資産	無形資産を含む
株主利益を重視	ステークホルダーとの関係を重視
方針がないか，あっても抽象的	方針が具体的
経理・財務・内部監査部門が担当	各部門が担当
属人的	プロセス重視
共通言語なし	共通言語によるリスクコミュニケーション
個別・断片的	総合的
事後対策型（場当たり的，対症療法的）	事前予防型（計画的）
事例分析型	環境変化対応型

出所：DeLoach（2000），pp. 15－16などを参考に筆者が作成。

図表2

リスクマネジメントの歴史

	第一期	第二期	第三期
対象とするリスク	非事業リスク[14]		事業リスクを含む
対策（Solutions）	保険	防止	
焦点（Focus）	内部		内部と市場
戦略（Strategy）	コーディネーションなし		システム的

出所：Sadgrove（2005），p. 2のFigure 1-1を筆者が修正。

に対処することである。リスクには「未知（unknown）のリスク」「未知の既知（known unknown）のリスク」「未知の未知（unknown unknowns）のリスク」がある[13]。ERMではシナリオ分析により未知のリスクが既知のリスクとなることもあるし，「未知の未知」のリスクに対しては，危機管理や事業継続計画により，その影響を最小限にとどめることができる（Walker et al., 2002, p. 11）。

新旧パラダイムの特徴を比較すると図表1のとおりである。

米国におけるリスクマネジメントの発展に関しては，初期段階（1955～1965年），移行段階（1965年～1975年），国際化段階（1975年～）という三つの段階があったとされる（Snider, 1991，邦訳，pp. 153-166）。それに対して，現代的リスクマネジメントをもカバーする歴史区分を示すと図表2のとおりである（Sadgrove, 2005, pp. 1-2）。

第三期に特徴的なものとしては，たとえば1995年にオーストラリアとニュージーランドが世界で最初にリスクマネジメントの規格を作成したことがある。その1999年改訂版（AS/NZS 4360，1999年）では，リスクマネジメントは「組織のあらゆる活動，機能，プロセスに伴うリスクがもたらす損失を最小化するとともに，リスクがもたらす好機が最大になるよう，論理的，システム的に，状況の確定，リスクの特定・分析・評価，処理，監視，およびコミュニケーションを行うこと」と定義されている。

2-2. 内部監査のパラダイムシフト

リスクマネジメントは米国で生成発展したものであり，今日に至るまで米国は世界一のリスクマネジメント大国であるが，それは保険管理に始まり，その後も損害保険とは不即不離の関係にある「伝統的リスクマネジメント」のことである[15]。しかし，ことERMに関しては，米国においてもそれほど普及が進んでいるとはいえない[16]。

その米国で，ERMの導入に成功した先進的な企業がある。その事例研究においては，「内部監査人がERMの導入に重要な役割を果たした」との知見が得られている。内部監査人がERMを担うというのは，内部監査がリスクマネジメントの観点から行われることである。会計や業務の監査にリスクマネジメントの視点が加わるというのは，監査人が経営者の立場にたって業務の遂行をチェックし，評価することである。これはもっぱら客観的・規範的な評価を旨とする監査においては大きな発想の転換を伴うものであった（Walker et al., 2002, p. 27）。

つまり内部監査人がERMの実践を主導したという事例からいえることは，内部監査のパラダイムシフトがあってそれが可能になったか，もしくはそれによって内部監査のパラダイムシフトが生じたかということである。これは鶏と卵の関係のようなものであり，要は両者の結びつきがパラダイムシフトであった。内部監査における新旧パラダイムを対比すると図表3のとおりである。

前述のとおり，内部監査とは内部統制の有効性を評価・保証するものであった。それがビジネス・リスクマネジメントに焦点を当てるものに変化した。その結果，新パラダイムの内部監査はERMの特徴をそのまま内包するものとなった。たとえば，「事後対応的」なものから「同時進行的」なものとなり，リスク評価が「リスク要因」から「シナリオ計画」中心のものとなり，内部監査報告書が「コントロール手続き」よりは「プロセス・リスク」に関するものになった。

さらに内部監査の役割が「独立の評価機能」か

図表3

内部監査のパラダイムシフト

旧パラダイム	新パラダイム
「内部統制」に焦点を当てる	「ビジネスリスク」に焦点を当てる
「検証機能」が中心	「検証機能」＋「コンサルティング機能」
事後対応的	同時進行的
一方的	相互作用的
断続的監視	継続的監視
経営管理の一部（戦略を観察）	経営戦略と一体化（戦略へ参加）
「リスク要因」中心のリスク評価	「シナリオ計画」重視のリスク評価
改善勧告は「内部統制」 • 強化 • 費用対効果 • 効率性・有効性	改善勧告は「リスクマネジメント」 • リスクの回避・分散 • リスクの共有・移転 • リスクのコントロール・受容
「機能的統制手続」志向の報告書	「プロセス・リスク」志向の報告書
役割は「独立の評価機能」	役割は ERM とコーポレートガバナンス

出所：McNamee（1998），p 5 を筆者が一部修正して作成。

ら「ERM とコーポレートガバナンス」へと変化した。そして本来，独立であるべき内部監査において，経営戦略への関与が生じた。こうした「戦略整合性」が両者のパラダイムシフトに共通する特徴である。それはリスクマネジメントであれ，内部監査であれ，付加価値を高めるためには戦略的な取り組みが不可欠であったからである。

その背景にあったのは，IT 化，グローバリゼーション，金融技術の進化，規制の変化，事業の合併・再編，組織構造の変化，消費者意識の変化など（Barton et al., 2002, pp. 2–3），あるいは「プロダクト型市場経済」から「ファイナンス型市場経済」への変化など（古賀，2003, pp. 3–4）の事業環境の変化である。

そのようなニューエコノミーの下で，株主価値[17]の増大が企業の至上命題となり，リスクマネジメントの目標は株主価値の維持，向上，創造となり，内部監査も同様にその存在意義を付加価値の向上に求めた。その結果，リスクマネジメントにおいては戦略的な性格が一段と強まり，内部監査においてはリスクアプローチが採用されることになったのである。

3. 触媒としてのコーポレートガバナンス

3-1. コーポレートガバナンスの役割

リスクマネジメントと内部統制と，それぞれの分野で生じたパラダイムシフトには通底するものがあることをみたが，コーポレートガバナンスはより直接的に両者を結び付けるものである。それはコーポレートガバナンスの中で内部統制とリスクマネジメントが重視されることになった，すなわちコーポレートガバナンスを実効あらしめるためには，内部統制とリスクマネジメントがともに必須のものとされたからである[18]。

コーポレートガバナンスとの関連で，内部統制とリスクマネジメントの融合を鮮明に打ち出したのは英国のターンバル・ガイダンスである。英国では一連の企業不祥事を契機として，1990 年代にコーポレートガバナンスに関する報告書が相次いで公表された[19]。それらの報告書は 1998 年に統合されて統合規定（The Combined Code, 1998）となった。統合規定には Good Governance の原則と Best Practice の規定が盛り込まれて，取締役会の責任において内部統制のシステムを確保すべきであるとされた。

統合規定を実践するためのガイダンスとして英国証券取引所と英国・ウェールズ勅許会計士協会が策定したのがターンバル・ガイダンス（1999 年）である。ターンバル・ガイダンスの眼目はリスクマネジメントを重視していることであり，リスクマネジメントを経営者および取締役会の責任とし，内部統制はリスクマネジメントにも重要な役割を果たすものとしていることである（後

藤，2001, p. 41）。

同様の動きはわが国においてもあり，2003年6月，経済産業省の「リスク管理・内部統制に関する研究会」が「リスク新時代の内部統制―リスクマネジメントと一体となって機能する内部統制の指針―」を，2005年7月には，経済産業省の「企業行動の開示・評価に関する研究会」が「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組について―構築及び開示のための指針―（案）」を公表した。

米国では，内部監査のパラダイムシフト（リスクアプローチへの転換）が正式に認知されたのは，1999年6月，内部監査人協会の理事会が以下の定義を承認したときである（Walker et al., 2002, p. 5）。

「内部監査は，組織体の運営を改善し，価値を付加するために行われる独立の客観的な保証およびコンサルティング活動である。内部監査は，リスクマネジメント，コントロールおよび組織体の統治プロセスの有効性を評価し，改善するための体系的で規律のとれたアプローチによって，組織体の目標の達成に貢献する」。

またコーポレートガバナンスとの関係については，1999年に全米取締役協会が「監査委員会に関するブルーリボン委員会報告」において組織の最高レベルでのリスクマネジメントの重要性を指摘している（Walker et al., 2002, p. 4）。

3-2. 「内部統制の統合的枠組み」（COSO1）と「全社的リスクマネジメント」（COSO2）

内部統制の「内部」は事業体の組織内部のことである。「統制」は一般的には「定められた目的に対して影響を及ぼすこと」であり「命令」「指示」「抑制」「規制」「管理」などが含まれる（COSO, 1992, 邦訳, pp. 175-176）。組織あるいは経営において「統制」が必須の機能であることはいうまでもない。

その内部統制は，監査の遂行を効率化させるという意義が認められて1940年代の初頭には，内部統制に関する報告書や指針および基準が数多く公表された。その後，1970年代の後半には，ウォーターゲート事件により不正防止の側面に焦点があたり，1977年海外不正支払防止法が制定され，1992年にトレッドウェイ委員会組織委員会による『内部統制の統合的枠組み』（以下COSO1）が公表された（COSO, 1992, 邦訳, pp. 157-165）。

COSO1が内部統制に関し各国のモデルとなったのは，3つの目的（①業務の有効性と効率性，②財務報告の信頼性，③関連法規の遵守）と，5つの構成要素（①統制環境，②リスクの評価，③統制活動，④情報と伝達，⑤監視活動）からなる定義を樹立し，同時に，内部統制の目的との関係において企業の内部統制を評価するための枠組みを提示したからである。

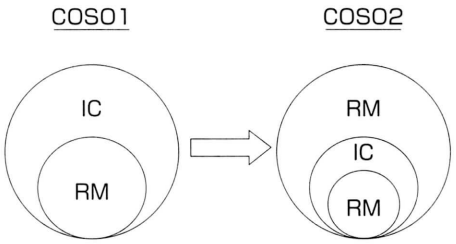
COSO1は，①内部統制を事業体の取締役会，経営者およびその他の人々によって遂行されるプロセスであるとしたこと，②取締役会や経営者に言及することによってコーポレートガバナンスとの接点を確保していること，③統制目的として「法令等の遵守」を明記していることの三点において画期的なものである（鳥羽，2005, p. 6）。

これらの点からいえるのは，COSO1は，前述した内部監査とリスクマネジメントにおけるパラダイムシフトを背景とするものであり，ターンバル・ガイダンスにおける内部統制とリスクマネジメントの融合につながるものであるということである。

内部統制とリスクマネジメントの融合に関してさらに象徴的なのは，COSOが2004年にCOSO2を公表したことである（図1参照）。COSO1ではリスクマネジメントは5つの構成要素の1つであった。しかしそれは「リスクをベースにして」とか「リスクアプローチによる」といった言い方がされるように，リスクマネジメントの思考方法によって内部統制を行うということである。その意味ではエンロン後になってようやく[20]，「リスクマネジメントの枠組みにおける内部統制」とされるに至ったのは当然のことである。

ちなみにCOSO2ではCOSO1の3つの目的の上位に「戦略」の目的が追加されている。これはERMの特徴である「戦略適合性」を具現するも

図表4
COSO 1 と COSO 2 の関係



のであり，リスクマネジメントと内部統制のパラダイムシフトにおいて顕著であった戦略性（価値創造経営）への傾斜と同一線上にあるものである。

COSO2 の図は，この論文において提示したリスクマネジメントと内部統制の関係を表したものである（図表4参照）。リスクマネジメントは内部統制の一部であるとする説（The Securities and Exchange Commission）と，逆に内部統制はリスクマネジメントの一部であるとする説（The Federal Deposit Insurance Corporation）がある（Chorafas, 2000, pp. 10–12）。しかし COSO2 が示唆するのは，リスクマネジメントは内部統制の一部であると同時に，その全体を大きく包摂するものでもあるということである。

3-3. 内部統制に関する2つの法律

わが国では，2006年5月1日，大会社に内部統制を義務付けた新会社法が施行され，2008年4月以降は，上場会社に財務報告の信頼性に関する内部統制を義務付ける金融商品取引法が施行される。前者は業務全般に法令順守などを徹底するための体制を，後者は財務報告を正確に行うための体制を求めるものである。

新会社法の考え方は「ファイナンス分野」「ガバナンス分野」「会計法制」などで起きている世界的な変化に整合するものであり（神田，2006, pp. 42–46），ガバナンス面での特徴は，①組織形態と組織再編の自由度を高め，②機関設計の自由度を高め，③それらと引き換えに経営の透明性と説明責任の向上を求め，④会計の適正化の確保を求め，そして⑤大会社における内部統制システムが適正に機能することを求めたことである（神田秀樹「新会社法と金融商品取引法　公正な市場へ統合視野に」『日本経済新聞』2006年9月5日）。

現行法のもとでも，委員会等設置会社の場合には内部統制システムの整備が義務付けられており，また裁判例によっても，たとえば大和証券株主代表訴訟事件大阪地裁判決（平成12年9月20日判決，資料版『商事法務』199号，p. 248）[21]や神戸製鋼株主代表訴訟事件所見（平成14年4月5日和解成立，旬刊『商事法務』1626号，p. 52）において，内部統制は取締役会の責任とされていた。したがって内部統制自体は新しいものではない。

金融商品取引法は，日本版SOX法とも言われるように，米国のサーベンス・オクスレー法（以下SOX法）に相当し，株式市場の信頼性を確保するためのものである。SOX法（別名「企業改革法」）は，エンロンなどの不正会計事件への反省から2002年7月に生まれた連邦法である。経営者には自ら内部統制を構築して評価する責務があるとし，CEOとCFOにはすべての財務報告への署名を義務付け，その後に不正事件が発生すれば厳罰を課すというものである。

以上のような背景と目的からして，同じ内部統制に関する規制であっても，2つの法律にはかなりの相違がある。会社法の対象となるのは資本金5億円以上あるいは負債200億円以上の大会社と委員会設置会社であり，その数は1万社以上になる。具体的な方法は各企業に委ねられており，法律が定めているのは，①取締役会で「内部統制に関する決議」を行うことと，②法施行後2回目の定時株主総会に提出する事業報告（ウェブサイトも可）でその「決議内容を開示」することである[22]。

会社法については，すでに多くの会社で，企業規模や社内の事情に応じた取り組みがなされているが，たとえばソニーでは，取締役会決議を公表し，監査委員会を補佐する専任スタッフを3人置いて，内部監査部門と連携して，国内外のグループ会社の監査を実施している（日本経済新聞，2006年8月17日）。

金融商品取引法が求めるのは，①有価証券報告

書に誤りがないことを保証する「確認書」の提出と，②正確な財務諸表を作成するための体制があるかどうかを点検し，自己評価する「内部統制報告書」の作成である[23]。とくにこの内部統制報告書については，2009年3月期から公認会計士もしくは監査法人の監査を受けることも義務付けられている。

内部統制報告書の作成に際しては，財務諸表を作成するための手続きに関して，そのリスクを特定して対策を講じる必要がある。SOX法への対応を行ったTDKの場合，国内外の連結子会社33社も含めて洗い出したリスクは約5,000件，対策は1万件以上（1つのリスクに複数の対策がありうる）にのぼり，2年半を要した（日本経済新聞，2006年1月30日）。

ちなみに，内部統制の体制構築に必要となるのは社内手続きの文書化であり，米国企業の多くはその準備に8ヶ月から1年の時間と平均5億円のコストを要し，わが国でも日本版SOX法関連の市場規模は2008年に7,000億円とみられている（日本経済新聞，2006年1月1日）。

会社法と金融商品取引法で共通するのは，いずれの内部統制においても，コーポレートガバナンス，すなわち株主の視点が確保されていることである。会社法では，決議内容の「株主への開示」を義務付けており，金融商品取引法はそもそもが「株主を保護」するための法律である。いずれの場合もキーワードは情報開示（ディスクロージャー）であり，金融商品取引法による内部統制を「ディスクロージャーの内部統制」とすれば，新会社法による内部統制は「内部統制のディスクロージャー」であるとされる所以である（長谷川，2005, pp. 8–10）。

4. 内部監査とERMの実践

米国・カナダの企業におけるERM導入のプロセスと内部監査の果たした役割に関して参考になるのは，Barton et al.（2002）の*Making Enterprise Risk Management Pay off*と，Walker et al.（2002）の*Enterprise Risk Management: Pulling it All Together*である。いずれも同じ3人（3人とも会計学博士および公認会計士）の共著による事例研究の姉妹書である。

内部監査のパラダイムシフトについて示唆するところがあるのはもっぱら後者であるが，前者もERMとは何か，リスクマネジメントにおけるパラダイムシフトとは何かを具体的に知る上で有益であるので，はじめにその概要を記しておきたい。

Barton et al.（2002）が対象としたのは，チェース・マンハッタン，デュポン，マイクロソフト，ユナイテッド・グレイン・グロワーズ（以下UGG），ユノカルの5社である。5社とも独自の方法でERMの導入に取り組んでいる先進的な企業である。ERM採用の必然性ともいえる会社のプロフィールも含めて，ERMの体制とERMの特徴を一覧表にまとめたのが図表5である。

5社の事例から浮かび上がるERMの特質は以

図表5

ERMの体制と特徴（その1）

	プロフィール	体制	特徴
チェース・マンハッタン	市場・信用リスクに強み	ERM委員会	VaR，ストレステストなどの組み合わせ，1988年にSVAを導入
デュポン	創業はダイナマイト	ERM委員会	コンサルタントを起用，EARを共通言語とする
マイクロソフト	イントラネット	財務部長 RMグループ	VaR，ストレステスト，非金融リスクにはシナリオ分析
UGG	穀物生産高の不確実性	ERM委員会	コンサルタントを起用，リスクの定量化
ユノカル	石油・ガス探鉱の不確実性	内部監査部門 安全環境部門	内部監査部門がERMの実行を支援，ただしERMはライン機能

出所：Barton et al.（2002）の内容に基づき筆者が作成。

図表 6

ERM の体制と特徴（その 2）

	最高監査責任者	タイトル	内部監査→ERM への道
カナダポスト	Carmen Lapointe Young	Corporate Auditor	リスクとコントロールの評価を指示された。独自の ERM プロセスを開発。
ファーストエナジー	Dave Richards	Audit Chief	内部監査をコンサルティング型に変更。問題解決策を提案。
ゼネラル・モーターズ	Jacqueline Wagner	General Auditor	ERM の信奉者。 Wagner が全体の責任者（owner）。
ユノカル	Karl Primm	General Auditor	内部監査をリスクベースへ変更。 ERM コンサルタントを 2 名雇用。
ウォルマート	John Lewis	Chief Audit Executive, VP	内部監査部門の Best Practice を採用。 サイロ型→統合アプローチへ変更。

出所：Walker et al.（2002, p. 13）の Figure 2. 1 を筆者が修正。

下のとおりである。①どの企業にも適用できる決まったやり方というものはない[24]。②トップの関与（コミットメント）が不可欠である。③スタッフ機能ではなくライン機能である（それが「全社的」の意味）。④組織や手続きというよりはネットワークとプロセスの問題である。⑤リスクの定量化が重要な役割を担う[25]。⑥ ERM を組織の統合原理とする。

内部監査人が ERM を主導した事例のみを集めているのは，後者の Walker et al.（2002）である。Barton et al.（2002）と同様に 5 社の事例を取り上げているが，ユノカルは前者と重複している。内部監査人の役職名，ERM にかかわることになった理由などを一覧表にしたものが図表 5 である。

なぜリスクマネージャーでなく内部監査人なのか。それは ERM が伝統的なリスクマネジメントとは非連続のものである，あるいは少なくともそのような一面があるからであり，内部監査人は，その業務が「リスク」と「コントロール」に関係しており，なおかつ事業の内容や目的について深い見識があるからである（Walker et al., 2002, p. 5）。

Walker et al.（2002）の事例研究から参考となるのは以下のような点である。

①同じ内部監査人によるものであっても，その実践の内容は一様ではない。それは ERM が企業文化や既存のマネジメントシステムなど「すでにあるもの」の上に構築されるべきものだからである（Walker et al., 2002, p. 32）。

②内部監査人の役割は ERM を促進させること（facilitation）であり，自らが ERM の責任者（process owner）となることは通常はない（Walker et al., 2002, p. 19）。

③内部監査人がリスクの評価をすることはない。リスクの評価は現業部門（subject matter expert）に任される（Walker et al., 2002, p. 19）。

④ ERM を社内に浸透させるための方法としては，リスクワークショップが一般的である（Walker et al., 2002, pp. 21–22）。ワークショップの司会進行は，ERM コンサルタントか，内部監査人が学習をして行う（Walker et al., 2002, p. 198）

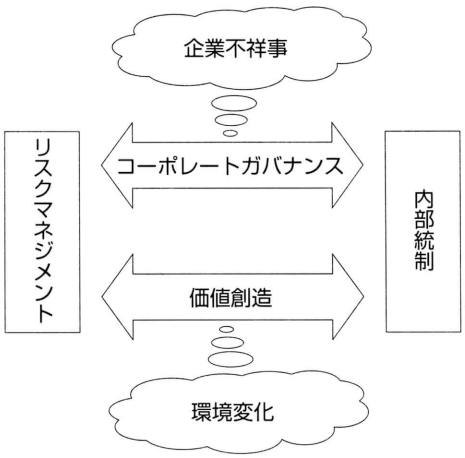
⑤内部監査人は ERM の報告を取締役会（監査委員会）に対して行う（Walker et al., 2002, pp. 26–27）。

最後に，内部監査と ERM に関して言えるのは，①古くからの問題を見るのに現代的な方法をもってすること，②経営の効率性と有効性を大きく改善すること，③不確実性に対処するための道を指し示すこと，そして④思考法と固定観念の転換を必要とすることである（Walker et al., 2002, p. 141）。

5. むすびにかえて

リスクマネジメントと内部統制の関係について，敢えて「融合」という言葉を使用したのは，それぞれの来歴を経て発達したリスクマネジメントと

図表7
リスクマネジメントと内部統制の関係



内部統制が，お互いを欠くべからざるものとして有機的に合体している，その関係がきわめて重要であると考えるからである。

両者を結合させることになったのは，一つには，事業環境の変化を背景とする「価値創造経営」への傾倒であり，もう一つは，絶えることのない企業不祥事によって高まった「コーポレートガバナンス」への希求である（図表7参照）。

内部統制はリスクアプローチ型へ，リスクマネジメントは価値創造型へと変化するパラダイムのシフトがあった。これは，内部統制はリスクマネジメントを通して，価値創造へつながるということである。つまりリスクマネジメントは内部統制の付加価値を高めるものであるといえる。

それではリスクマネジメントにおける内部統制の意義は何であろうか。それはリスクマネジメントの実践に有益であることである。ERMの普及において，内部統制は奇貨ともいうべきものではないかと考えられる。内部統制が法制化されたということは，それと一体の関係にあるリスクマネジメントも法的に強制されるということである[26]。

事例研究の企業においても，そのERMはまだ「旅の途中」であると言われる（Walker et al., 2002, p. 12, p. 28）。ERMの実践が容易でないのは，それが「リスクマネジメントを日常業務に組み込み特別な仕事としない」ということだからである（後藤，2001, p. 35）。それは突き詰めれば企業文化の問題であり，経営トップ（米国ではChief Executive Officer, Chief Financial Officer, Chief Risk Officer, Chief Audit ExecutiveなどいわゆるCレベルの役員）の意識改革とリーダーシップなしには成り立たない。

そのことのアナロジーとしてあるのが日本型企業システムのサブシステムであるとされる「全社的品質管理」である[27]。それは現場の品質問題は，品質管理の専門スタッフではなく，現場の社員で解決する，そのために品質管理を社員全員のものにするということであった。ここで「品質管理」を「内部統制」に置き換えることができるなら，それは「日本型内部統制」となるであろう[28]。

米国では，SOX法は厳格すぎるということで，規制緩和への揺り戻しの動きがある。わが国においても内部統制が機能するかどうか，それが企業の価値創造に有効かどうかは，リスクマネジメントと内部統制の関係がどう生かされるか，内部統制の実務にERMのプロセスをどれだけ十分に組み込むことができるかによるであろう。

注

1）経済産業省（2003, p. 11, p. 13）では，内部統制は「リスクマネジメントを支えるもの」としている。注18も参照。

2）内部統制の定義は，①The Committee of Sponsoring Organization of the Treadway Commission（COSO），②The Institute of Certified Public Accountants（AICPA），③The Institute of Internal Auditors（IIA），④The Basle Committee of Banking Supervision，⑤The European Monetary Institute（EMI）の間でも互いに矛盾するところがある（Chorafas, 2000, pp. 8-9, pp. 255-258）。

3）同様の指摘について五十嵐（2003, p. 111）参照。

4）内部統制の概念は時代により変化しており，松井（2006, pp. 27-30）は，COSO1（注6参照）以前の状況につき，1936年アメリカ会計士協会の定義，1949年同協会の定義，および1988年アメリカ公認会計士協会の定義を，それぞれ「狭義の理解」「広義の理解」「最広義の理解」の例として挙げている。1936年定義は監査人の，1949年定義は経営者の観点からのものであり，1988年定義では，統制（経営）環境を含めて説明するものとなった。

5）両者の関係は内部統制の定義とともに，リスクマネジメントをどう捉えるかにもよる。リスクマネジメントの定義については後述するが，仮にリスクを「経営目的の達成を不確実にしたり，阻害する要因」

とし，内部統制を「設定した経営目的の達成を管理する仕組みないしプロセス」とすれば，内部統制はリスクマネジメントの一部であるということになる（森本他，2005, p. 78）。

6）トレッドウェイ委員会組織委員会（The Committee of Sponsoring Organizations of The Treadway Commission—以下 COSO）が1992年9月に公表した『内部統制の統合的枠組み』を COSO1，2004年9月に公表した『全社的リスクマネジメント—統合的フレームワーク』（八田監訳，2006）を COSO2 と表記する。

7）保険とリスクマネジメントの関係については Doherty（2000, pp. 4-6）参照。

8）ISO DGUIDE 73, *Risk management-Vocabulary-Guidelines for use in Standards*, Aug. 31, 2001.（財）日本規格協会編（2003, pp. 85-104）参照。

9）McNamee（1998, p. 2, p. 125）は多数の文献をレビューした結果，「経営と戦略」の文脈においては，これがリスクの最大公約数的な定義であるしている。

10）リスクの定義に関し，不確実性（uncertainty）には計測可能なものと計測不可能なものとの二種類があることを指摘し，前者をリスクとし，後者を不確実性と呼ぶことにしたのは Knight（1921, Chapter VII, VIII）である。リスクは管理が可能であるが，不確実性は当事者である企業のみが特別の洞察をもつことができるものであり，利益と損失の源泉であるとした。

11）ビジネスリスクはたとえば，戦略リスク，金融リスク，オペレーショナル（操業）リスク，ハザード（危険）リスクに分類される（Walker et al., 2002, p. 3）。注14も参照。

12）リスクの最適化（optimization of risk）とは，リスクのマイナスの影響を最小化し，プラスの影響を最大化することであり，現代的リスクマネジメントを特徴付ける重要な概念の一つである（上田，2003, p. 34）。

13）原文は，“There are knowns, known unknowns, and unknown unknowns（作者不詳）.”「未知の既知」とは「知らないことを知っていること」，「未知の未知」とは「知らないということも知らないこと」である（Walker et al., 2002, p. 11）。

14）Sadgrove（2005, p. 3）はビジネスリスクを事業リスク（entrepreneurial risk）と非事業リスク（non-entrepreneurial risk）に二分類する。前者が投機的リスク，後者が純粋リスクに相当するものである。

15）2005年の損害保険料で比較すると米国は6,258億ドル（世界占有率43.10%），日本は1,005億ドル（6.92%）であり，米国は日本の6.2倍である（Swiss Re, *sigma* No. 5 2006）。米国流のリスクマネジメントに関しては，杉野（2003, pp 153-154）参照。

16）米国・カナダで ERM を導入済みの企業の数は，KPMG の調査（2001年）では30%～35%，最近の Tillinghast-Towers Perrin の調査では，十分に採用済みが11%，部分的に採用済みが38%の合計49%であった（Rejda, 2005, p. 66）。

17）わが国では「企業価値」という言葉がよく使用されるが，米国には企業価値に当たる英語はない（森生，2006, pp. 73－74）。

18）これはコーポレートガバナンスを，「伝統的株主価値最大化モデル」「洗練された株主価値モデル」「多元主義モデル」（稲上，2000, pp. 11－28）のいずれにせよ，株主もしくはそのほかのステークホルダーが経営を規律付けるための仕組みと方法であるする定義によるもの，すなわちコーポレートガバナンスの仕組みを所与のものとして，それをいかに強化するかという立場の議論である。そもそもコーポレートガバナンスのないのが問題であるとの前提にたてば，リスクマネジメントとしてのコーポレートガバナンスや如何との問題提起もありうる（杉野，2005）。

19）The Cadbury Report 1992, The Greenbury Report 1995, The Hampel Report 1998 などがある。

20）Sadgrove（2005, p. 2）は COSO2 が作成された理由の一つはエンロンとアーサー・アンダーセンのスキャンダルであるとするが，COSO が COSO2 の策定を開始したのは2001年であり，エンロンなどのスキャンダルとはたまたま時期が重なったということのようである（八田監訳，2006, ix）。しかしリスクマネジメントの立場からいえば，遅きに失した感は否めない。

21）判決では「…会社経営の根幹に係わるリスク管理体制の大綱については，取締役会で決定することを要し，業務執行を担当する代表取締役及び業務担当取締役は，大綱を踏まえ，担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う」とされている。ここでいう「リスク管理体制」が「内部統制システム」であり，法律分野では「リスク管理」と「内部統制」は同義で使用される（神田，2006, p. 76）。

22）新会社法では，株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備（内部統制システムの構築）を求め（第362条4項6号），大会社である取締役会設置会社はこれを取締役会で決定しなければならないとしている（同条5項）。

23）2006年6月に成立した金融商品取引法では，財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府で定める体制の確立，及び，その体制に関して内閣府令で定めるところにより評価した報告書（内部統制報告書）の提出を義務付けている（第24条4項4号）。

24）DeLoach（2000, p. xiii）によれば，“EWRM is not a ‘one-size-fits-all’ solution.”である。

25）金融機関における（あるいは金融リスクに関する）定量化の技術は一般の事業会社や非金融リスクにも移植されつつある（DeLoach, 2000, p. 13）。

26）2001年7月に KPMG が欧州8カ国，213の企業に対して行った調査がある。それによると，ターンバル・ガイダンスの結果，内部統制とリスクマネジメントの企業内への浸透が進んでいるかどうか，「非常にそう思う」との回答は英国で約20%，法律で強制されているドイツでは約70%であった（上田，2003, pp. 133-134）。

27）杉野（2003）参照。

28）牧野（2006, pp 217-218）参照。

参考文献

Barton, T. L., W. G. Shenkir and P. L. Walker（2002）

Making Enterprise Risk Management Pay off, Prentice-Hall（刈屋武昭・佐藤勉・藤田正幸訳『収益を作る戦略的リスクマネジメント』東洋経済新報社，2003年）.

Chorafas, D. N.（2000）*Reliable Financial Reporting and Internal Control: A Global Implementation Guide*, John Wiley & Sons.

COSO（The Committee of Sponsoring Organizations of the Treadway Commission）（1992）*Internal Control-Integrated Framework*（鳥羽至英・八田進二・高田敏文訳『内部統制の統合的枠組み（理論篇）（ツール篇）』白桃書房，1996年）.

COSO（The Committee of Sponsoring Organizations of the Treadway Commission）（2004）*Enterprise Risk Management-Integrated Framework: Executive Summary and Framework*（八田進二監訳・中央青山監査法人訳『全社的リスクマネジメントフレームワーク篇』東洋経済新報社，2006年）.

Culp, C. L.（2001）*The Risk Management Process: Business Strategy and Tactics*, John Wiley & Sons.

DeLoach, J. W.（2000）*Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity*, Pearson Education.

Doherty, N. A.（2000）*Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*, McGraw-Hill.

長谷川俊明（2005）『新会社法が求める内部統制とその開示』中央経済社。

五十嵐達朗（2003）「企業経営のインフラストラクチャーとしての内部統制」監査法人トーマツ編『リスクマネジメントと内部統制』税務研究会出版局，pp. 107-134。

稲上毅（2000）「新日本型コーポレート・ガバナンスと雇用・労使関係」稲上毅・連合総合生活開発研究所編著『現代日本のコーポレートガバナンス』東洋経済新報社，pp. 3-74。

神田秀樹（2006）『会社法入門』岩波書店。

企業会計審議会（2005）「財務報告に係る内部統制の評価及び監査の基準のあり方について」12月8日。

経済産業省（2003）「リスク新時代の内部統制—リスクマネジメントと一体となって機能する内部統制の指針」6月27日。

経済産業省（2005）「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組みについて—構築及び開示のための指針—（案）」7月13日。

Knight, F. H.（1921）*Risk, Uncertainty and Profit*, Houghton Mifflin（奥隅栄喜訳『危険，不確実性及び利潤』文雅堂銀行研究社，1959年）。

古賀智敏（2003）「リスクマネジメントの理論的フレームワーク」古賀智敏・河崎照行編著『リスクマネジメントと会計』同文舘，pp. 3-15。

牧野二郎（2006）『新会社法の核心—日本型「内部統制」問題』岩波書店。

松井隆幸（2006）『内部監査（改訂版）』同文舘出版。

McNamee, D. and G. M. Selim（1998）*Risk Management: Changing the Internal Auditor's Paradigm*, The Institute of Internal Auditors Research Foundation.

森生明（2006）『会社の値段』筑摩書房。

森本親治・守屋光博・高木将人（IBMビジネスコンサルティングサービス）（2005）『企業改革法が変える内部統制プロセス』日経BP社。

後藤和廣（2001）「企業経営の重要課題となったリスクマネジメント—英国のリスクマネジメント効果開示要求とコーポレート・ガバナンス—」『損害保険研究』第62巻第4号，pp. 31-71。

㈶日本規格協会編（2003）『JIS Q 2001：2001 リスクマネジメントシステム構築のための指針』財団法人日本規格協会。

Rejda, G. E.（2005）*Principles of Risk Management and Insurance*, 9th Edition, Pearson Education.

Sadgrove, K.（2005）*The Complete Guide to Business Risk Management*, 2nd Edition, Gower Publishing.

Snider, H. W.（1991）"Risk Management: A Retrospective View." *RIMS*, Vol. 38. No. 4, pp. 47-54（森宮康訳「リスク・マネジメント回顧録」『損害保険研究』第53巻第4号，1992年，pp. 153-166）.

杉野文俊（2003）「現代的リスクマネジメントの可能性に関する一考察—日本型品質管理との類似性について」『保険学雑誌』第582号，pp. 152-172。

杉野文俊（2005）「リスクマネジメントとコーポレートガバナンスに関する一考察—「経営者リスク」のリスクマネジメントについて」『専修大学商学研究所報』第37巻第2号。

鳥羽至英（2005）『内部統制の理論と実務—執行・監督・監査の視点から（普及版）』国元書房。

上田和勇（2003）『企業価値創造型リスクマネジメント—その概念と事例』白桃書房。

Walker, P. L., W. G. Shenkir and T. L. Barton（2002）*Enterprise Risk Management: Pulling it All Together*, The Institute of Internal Auditors Research Foundation（刈屋武昭監訳『戦略的事業リスク経営』東洋経済新報社，2004年）.

Williams, C. A. and R. M. Heins（1976）*Risk Management and Insurance*, 3rd Edition, McGraw-Hill（武井勲訳『リスク・マネジメント（上）』海文堂，1978年）.